



Information Security Incident Management Standard

Document Name: Information Security Incident
Management
Document ID: IS.009

Effective Date: October 15th, 2018
Last Revised Date: October 4th, 2018

Table of contents

1. Purpose.....	2
2. Authority	2
3. Scope	2
4. Responsibility	2
5. Compliance	2
6. Standard Statements.....	3
6.1. Incident Response Program.....	3
6.2. Security Incident Response Team (SIRT)	3
6.3. Incident Identification, Investigation and Analysis	4
6.4. Incident Reporting and Escalation	5
6.5. Security Incident Response and Investigation.....	7
6.6. Collection of Evidence	8
6.7. Post- Incident Analysis	8
7. Control Mapping.....	9
8. Related Documents	9
9. Document Change Control.....	9

1. PURPOSE

- 1.1. The **standard** documents the requirements for managing an information security **incident**; describes the actions to be taken should an **incident** occur; and details each phase of the **incident** management life cycle, including identification, investigation, response and remediation.

2. AUTHORITY

- 2.1. M.G.L. Ch. 7d provides that “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.”

3. SCOPE

- 3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus.. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their personnel comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

- 4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this **standard**.
- 4.2. The Enterprise Security Office is responsible for this **standard** and may enlist other departments to assist in the monitoring and maintenance of compliance with this **standard**.
- 4.3. Any inquiries or comments regarding this **standard** shall be submitted to the Enterprise Security Office by sending an email to [EOTSS-DL-Security Office](#).
- 4.4. Additional information regarding this **standard** and its related standards may be found at <https://www.mass.gov/cybersecurity/policies>.

5. COMPLIANCE

- 5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office([EOTSS-DL-Security Office](#)). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1. **Incident** Response Program

The Enterprise Security Office shall be responsible for developing a program to effectively detect, respond and resolve **incidents** that affect the security of the Commonwealth's **information assets**.

6.1.1. The **incident** response program shall entail:

- 6.1.1.1. Documented process that defines the **incident** response life cycle.
- 6.1.1.2. Definition of roles and responsibilities for internal and external stakeholders, including the formal establishment of a Security **Incident** Response Team.
- 6.1.1.3. Formal event reporting and escalation procedures.
- 6.1.1.4. Tools and enablers to facilitate **incident** management.

6.2. Security **Incident** Response Team (SIRT)

6.2.1 The roles and responsibilities for the members of the core and extended SIRT team must be clearly defined.

6.2.1.1 The **Incident** Response Coordinator (i.e., Commonwealth CISO or designee) shall:

- 6.2.1.1.1 Oversee and provide guidance and direction to the **incident** response team.
- 6.2.1.1.2 Serve as a communication liaison to internal and external entities, including Enterprise Security Office leadership, the agency leadership and other relevant stakeholders.
- 6.2.1.1.3 Validate the results of response actions.
- 6.2.1.1.4 Coordinate the development of training plans for the **incident** response plan.
- 6.2.1.1.5 Sponsor periodic (i.e., annually recommended) tabletop exercises to test **incident** response readiness.
- 6.2.1.1.6 Sustain, maintain and improve the **information security incident** response process.
- 6.2.1.1.7 Maintain compliance with record retention requirements.

6.2.1.2 The **Incident** Response Lead shall:

- 6.2.1.2.1 Oversee response efforts for a specific information security **incident**. (Note: Every **incident** may have a different IR Lead).
- 6.2.1.2.2 Serve as the escalation/communication liaison between the SIRT team and information security leadership as well as other relevant stakeholders.
- 6.2.1.2.3 Act as or engage the appropriate subject matter resources when key decisions need to be made during the information security **incident** response process.

6.2.1.3 The **Incident** Response Analyst (i.e., subject-matter resources) shall:

- 6.2.1.3.1 Ensure investigations are conducted in accordance with documented procedures and that evidence is handled appropriately.
- 6.2.1.3.2 Collect, process and maintain information security **incident** information.
- 6.2.1.3.3 Manage information security **incident** status documentation.
- 6.2.1.3.4 Communicate and escalate **incidents**, as required.
- 6.2.1.3.5 Manage security **incidents** through post-**incident** review.

6.2.2.4. The extended **incident** response team includes cross-functional resources that will provide support as appropriate.

- 6.2.2.4.1. Digital Forensics Service Provider: Maintains a forensics service provider on retainer to assist with the recovery and investigation of information in digital formats as needed.
- 6.2.2.4.2. Legal: Provides advice regarding liability issues if an **incident** affects customers or third parties, or may lead to litigation.
- 6.2.2.4.3. Human Resources: Provides advice on managing **incidents** that involve **personnel**.
- 6.2.2.4.4. Public Relations/Communications: Communicates the details of security **incidents** to external stakeholders, including state and federal law enforcement and regulators. Manages crisis communication.

6.3. **Incident** Identification, Investigation and Analysis

6.3.1. Defining potential information security **incidents**

A security **incident** is defined as any event which has the potential or has already resulted in the unauthorized acquisition, misappropriation, use or manipulation of information that compromises the confidentiality, integrity or availability of the Commonwealth's **information assets**. Examples include, but are not limited to:

- 6.3.1.1. Unauthorized and illegal disclosure, destruction and/or alteration of files, Commonwealth IT systems and information, including **confidential information**.
- 6.3.1.2. Unauthorized use of a Commonwealth IT system for the transmission, processing or storage of information.
- 6.3.1.3. Changes to system hardware, firmware or software characteristics intentionally concealed from the IT **Information Owner** and made without their knowledge or consent.
- 6.3.1.4. Detection of malware or malicious code (viruses, worms, etc.).
- 6.3.1.5. Unauthorized probes, scans or sniffers on the Commonwealth's internal network.
- 6.3.1.6. Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.
- 6.3.1.7. Harassment and threats conducted via Commonwealth email resources.

- 6.3.1.8. Web page defacement, unauthorized use of system privileges and attempts (either failed or successful) to gain unauthorized access to a system or its information.
- 6.3.1.9. Legal or regulatory violations involving Commonwealth **information assets**.
- 6.3.1.10. Violation of the Commonwealth's information security policies.
- 6.3.1.11. Cyber-stalking, identity theft or child pornography.
- 6.3.1.12. Unauthorized physical access to a secure area (e.g., data centers).
- 6.3.2. Per the *Logging and Event Monitoring Standard*, security alerts from security monitoring systems, including but not limited to intrusion detection and prevention, firewalls, email and file-integrity monitoring systems shall be collected and monitored.
 - 6.3.2.1. The Security Operations Center (SOC) shall analyze log information from security monitoring systems to establish a baseline of events expected for the normal system and network operations. Commonwealth Executive Offices and Agencies must ensure that any exceptions from these baseline events shall be reported to the responsible **Information Owner**.
 - 6.3.2.2. External feed sources, including resources from the Fusion Center, shall be leveraged to assist with the **incident** response process.

6.4. **Incident** Reporting and Escalation

Commonwealth Executive Offices and Agencies must establish, document, and distribute security **incident** response and escalation procedures to ensure timely and effective handling of **incidents**.

6.4.1. Information security **incident** impact rating

Impact	Characteristics	Response time ¹	Notification Level	Post-incident report req.
High	Threat to human safety. Adverse impact on a "Critical" or "High" risk rated information asset, including infrastructure, applications and services (see <i>Asset Management Standard</i>). Financial or legal liability equal to \$1m and above to the Commonwealth. Potential compromise of information classified as confidential information , including PII and other regulated information.	Immediate	Risk Governance Committee, Commonwealth CIO, CISO and agency heads	Yes
Medium	Adverse impact on a "Medium" risk rated information asset, including infrastructure, applications and services (see <i>Asset Management Standard</i>). Financial or legal liability between \$1m and \$100,000. Potential compromise of information not intended for public disclosure.	4 hours	Commonwealth CISO, agency heads	Yes
Low	Adverse impact on a "Low" risk rated information asset,	Next	Technical support	No, unless

¹ Note: This is not resolution time but the start time of the incident response process.

	including infrastructure, applications and services (see <i>Asset Management Standard</i>). Financial or legal liability of less than \$100,000.	business day	for impacted information asset	decided otherwise by the IR Coordinator
--	--	--------------	--------------------------------	---

6.4.2. Information security **incident** reporting and escalation

6.4.2.1 Define regular metrics and reporting cadence to the appropriate audience.

6.4.2.2 Security **incidents**, whether potential or actual, shall be reported immediately to the helpdesk or Enterprise Security Office (*See contact information in Appendix*)

6.4.2.3 Commonwealth Executive Offices and Agencies must ensure that **personnel** are required to cooperate with the SIRT team by providing accurate and timely information.

6.4.2.4 As the first line of defense, Commonwealth Executive Offices and Agencies must ensure that **personnel** are responsible for reporting suspicious activities.

6.4.3. Management reporting and escalation

The SIRT team shall notify the Risk Governance Committee about security **incidents** that have an impact rating of "high." The report shall include (as applicable):

6.4.3.1. Date and time of notification

6.4.3.2. Type of **incident** detected

6.4.3.3. Description of the **incident**

6.4.3.4. **Incident** response status

6.4.3.5. Location

6.4.3.6. Affected systems

6.4.3.7. User groups affected

6.4.3.8. Recover time expectations

6.4.3.9. Internal and external stakeholder contacts that need to be notified

6.4.3.10. Identification, containment and eradication measures

6.4.3.11. Evidence collected

6.4.3.12. Pending actions (if any)

6.4.4. Communication protocols

All information pertaining to an **incident** investigation shall be handled with discretion and disclosed only on a need-to-know basis. **Incident** reports shall be categorized as **confidential** at the discretion of the Enterprise Security Office. The Commonwealth CISO shall be designated the owner for all **incident** investigation related documentation.

6.5. Security Incident Response and Investigation

The Enterprise Security Office with the relevant stakeholders must take appropriate steps to ensure proper documentation, investigation, risk analysis, impact analysis and containment measures are taken in order to minimize the risk to the Commonwealth once a security event is identified.

6.5.1. Incident response procedures

Commonwealth offices and agencies must document procedures for responding to security **incidents** to limit further damage to the Commonwealth's **information assets**. Procedures shall include:

- 6.5.1.1. Identification of the cause of the **incident**

- 6.5.1.2. Execution of corrective actions

- 6.5.1.3. Post-**incident** analysis

- 6.5.1.4. Communication strategy

6.5.2. Incident response plan

Commonwealth Offices and Agencies shall establish an **incident** response plan. The **incident** response plan shall include, at a minimum:

- 6.5.2.1. Roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of required internal and external parties.

- 6.5.2.2. Specific **incident** response procedures.

- 6.5.2.3. Execution of corrective actions and post-**incident** analysis.

- 6.5.2.4. Establish criteria to activate business recovery and continuity processes (*See Business Continuity and Disaster Recovery Standard*).

- 6.5.2.5. Data backup processes (*See Data Backup and Restoration in the Asset Management Standard*).

- 6.5.2.6. Analysis of legal requirements for reporting compromises.

- 6.5.2.7. Reference or inclusion of **incident** response procedures from required external parties.

Commonwealth Offices and Agencies shall establish a process to modify and evolve the **incident** response plan and procedures according to lessons learned. The **incident** response plan and procedures shall be tested at least annually.

6.5.3. Incident containment

- 6.5.3.1. The SIRT team shall confirm the validity of the reported **incident**, containing and minimizing the impact of the **incident** in collaboration with the relevant stakeholders.

- 6.5.3.2. The **information asset** should be removed or quarantined from all Commonwealth networks where technically feasible.

6.5.4. Incident investigation

The SIRT team shall perform the following as part of the **incident** investigation process:

- 6.5.4.1. Gather information regarding the situation and elements involved (e.g., log correlation analysis).
- 6.5.4.2. Determine the scope, severity, impact and nature of the **incident**.
- 6.5.4.3. Determine root cause.
- 6.5.4.4. Determine response and recovery timelines.
- 6.5.4.5. Contextualize the evidence collected and document facts of the **incident**.
- 6.5.4.6. Gather system events and/or audit records.

6.6. Collection of Evidence

Evidence in whichever form it exists (digital, physical, original or copied) may be collected. Evidence shall be collected and preserved in a manner that is consistent with legal and record retention requirements.

- 6.6.1. A file comparison utility shall be run to identify all changes to **information systems** (where applicable).
- 6.6.2. Log(s) shall be copied to separate media and stored appropriately.
- 6.6.3. The **information asset** shall be restored from trusted backup copies.
- 6.6.4. If there is an expectation that there may be legal implications, appropriate chain of custody requirements must be met. The SIRT team shall consult with Legal on whether a certified forensics professional is engaged.
- 6.6.5. Information describing all reported information security **incidents** shall be retained for a minimum of three (3) years or as determined by Legal.

6.7. Post-**Incident** Analysis

The post-**incident** analysis shall be conducted in a timely manner to determine the organizational impact and confirm the causes, motives of the attack, and any potential mitigating actions. The analysis shall include:

- 6.7.1. Post-**incident** inventory to account for all the **information systems** owned or managed by the Commonwealth that may have been impacted.
- 6.7.2. Assessment of the involved systems to ensure that once they are returned to service only those with access needs are granted access to the system.
- 6.7.3. Risk-analysis of critical systems based on knowledge acquired and lessons learned.
- 6.7.4. Based on lessons learned, policies, processes or controls should be reviewed to determine whether there are opportunities for improvement.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1. Security <i>Incident</i> Response Team (SIRT)	IR-1	-	ID.GV-1
	IR-2	-	-
	IR-8	-	PR.IP-7
		CSC 17	PR.AT-4
	IR-10	-	-
6.2. <i>Incident</i> Identification, Investigation and Analysis	RA-3	CSC 4	ID.RA-1
	RA-5	CSC 4	ID.RA-1
	SI-2	CSC 4	ID.RA-1
		-	PR.IP-9
		-	RS.AN - Family
	SI-5	CSC 4	ID.RA-1
6.3. <i>Incident</i> Reporting and Escalation	AU-6	CSC 6	PR.PT-1
	IR-1	-	ID.GV-1
	IR-6	CSC 19	RS.CO-2
	SI-4	CSC 4	ID.RA-1
	SI-5	CSC 4	ID.RA-1
	PL-4	-	-
	SI-2	CSC 4	ID.RA-1
	SI-4	CSC 4	ID.RA-1
	SI-5	CSC 4	ID.RA-1
		CSC 19	RC.CO-1
		CSC 19	RC.CO-2
		CSC 19	RC.CO-3
	IR-3	CSC 19	PR.IP-10
		-	RS.MI Family
6.4. Security <i>Incident</i> Response and Investigation	IR-4	-	DE.AE-family
	IR-6	CSC 19	RS.CO-2
		-	RS.CO Family
			RC.RP-1
6.5. Collection of Evidence	IR-6	CSC 19	RS.CO-2
	IR-7	-	-
	AU-2	CSC 6	PR.PT-1
	AU-6	CSC 6	PR.PT-1
	AU-7	CSC 6	PR.PT-1
6.6. Post- <i>Incident</i> Analysis	IR-4	-	DE.AE-family
		-	RS.IM - 1,2
	IR-5	CSC 6	DE.AE-3

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections and Formatting
0.95	Sean Vinck	5/7/2018	Corrections and formatting
0.97	Andrew Rudder	5/31/2018	Corrections and formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This *Information Security **Incident** Management Standard* document shall be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.